Developing Joint Information Operations Warriors

by James A. Pickle, Lieutenant Colonel, USAF

Editorial Abstract: The author focuses on the need for a dedicated IO career force for the DOD to truly achieve information dominance. His analysis begins with a quick review of joint IO doctrine, Service approaches to IO, and IO personnel management, followed by IO education and training challenges. He offers recommendations for improvement, to help ensure we can influence, disrupt, degrade, or deny an adversaries ability to make a coherent decision at a time of our choosing.

Sun Tzu might be considered the very first information operations warrior even if he didn't call it IO. He understood the importance of deception, of an integrated military strategy, and of a coherent message to his adversary. "To subdue the enemy without fighting is the acme of skill."[1] IO isn't new; what is relatively new is the formal Department of Defense (DOD) direction of IO as a core military competency. The new Joint Publication 3-13, *Information Operations*, states "IO are integral to the successful execution of military operations." Around the world "across a range of unusual battle-spaces —global computer networks, human psychology, and electronic systems"[2] —the DOD is engaged in IO. This new focus is driven by technological developments that allow information to be shared across distances, languages, and barriers inconceivable only a few years ago.

DOD is moving forward. In the last three years these policy and doctrine documents have been published or updated:

- *Classified Information Operations Roadmap*, Oct 03

- *Defense Planning Guidance* 04-09

-DOD Directive 5143.01, Under Secretary of Defense for Intelligence, Nov 05

- DOD Instructions (DODI) 3608.11, *Information Operations Career Force,* Nov 05

- DODI 3608.12, *Joint Information Operations Education,* Nov 05

- JP 3-13, *Information Operations,* 13 Feb 06

- *Quadrennial Defense Review,* Feb 06

These documents lay a joint doctrinal foundation for the DOD IO career field, and designate USD(I) as the functional proponent responsible for IO career force policy and oversight.[3]

Dedicated IO professionals are essential for DOD IO to provide information dominance. Beginning with the end in mind, how should the DOD grow a chief IO officer? How do we develop J-39s such as the Director for Global Operations, the Joint Staff, or US Strategic Command (USSTRATCOM)?[4] No adequate guidance currently exists. This research suggests to attain the full promise of DOD IO, we need a joint-level approach to train IO warriors. DODI 3608.11 and 12 establish the requirement to train an IO career force comprised of IO capability specialists and IO planners. But there are multiple challenges to meeting the USD(I) guidance. Having considered the dilemma, this analysis offers a few recommendations to get the most from limited funding, and allow the creation of a true joint IO warrior.

Laying the Information Operations Doctrinal Foundation

DPG 04-09 directed each service to develop an IO career force. The *IO Roadmap* provided amplifying guidance. DODI 3608.11 directs "an IO Career Force shall be established and maintained to plan and execute fully integrated IO."[5] DODI 3608.11 further defines two categories within the IO career force for both the Active and Reserve component: IO capability specialists and IO planners. An IO capability specialist is "a functional expert in one or more of the specialized core capabilities."[6] An IO planner is "a functional expert trained and qualified to plan and execute full spectrum IO."[7] The instruction further directs education, training, and experience standards be established and requires an annual update to the Secretary of Defense (Sec Def). The goal is to provide a DOD-wide, common foundation of IO knowledge and proficiency. [8]

DODI 3608.12 establishes a BOArd of Advisers (BOA) and BOA working group for joint IO education, with the Joint Staff and USSTRATCOM each providing a general officer as co-chairs. Further, Joint Forces Staff College (JFSC) is tasked to develop and conduct a joint IO planner course. The Naval Post Graduate School is tasked to establish an IO Center of Excellence and a graduate level joint IO education program.[9] The DODIs provide USD(I) intent for joint IO career force and education, but not program specifics. Detailed educational requirements are left to the BOA and the individual services.

The JP 3-13 IO definition identifies five core IO capabilities. IO is "the integrated employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[10] Along with the core capabilities, JP 3-13 identifies five supporting capabilities: information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. Supporting capabilities either directly or indirectly contribute to full spectrum IO. Also, three other military functions are related capabilities for IO: public affairs (PA), civil military operations (CMO), and defense support to public diplomacy. "These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting IO capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO."[11] Of note, the new JP 3-13 removes information warfare as a term from joint doctrine and discontinues use of the terms offensive and defensive IO, but retains that IO is applied to achieve both offensive and defensive objectives.[12]

What is the principal goal of IO? "To achieve and maintain information superiority for the US and its allies."[13] Put simply, information superiority enables decision superiority. Decision superiority allows our forces to observe, orient, decide, and act faster than our adversaries. To train IO warriors one must understand the battlespace—the information environment. IO gains information superiority by taking control of this realm "... Where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principle environment of decision making."[14] The information environment is comprised of "three interrelated dimensions: physical, information, and cognitive."[15] The physical dimension is easiest to measure, and the combat power dimension is traditionally applied. The information dimension consists of the content and flow of information, and must be protected. The cognitive dimension is the most important of the three because it encompasses the mind of the target audience (TA). Notably, it is the dimension of perception and eventual decisions.[16] IO impacts the decision maker by taking actions to add, modify, or remove information from an individual's environment, by affecting the infrastructure that supports the decision maker, or by influencing the way people receive, process, and use data and information.[17] Specific methods to influence a TA require focused training.

IO warriors in training. (US Army)

IO Core Capabilities

Each of the five IO core, supporting, and related capabilities have existed long enough for most joint and service organizations to establish, understand, and use the doctrine. We've practiced several of the capabilities for centuries. In the modern age, with our emphasis on information superiority, the US has added to the legacy capabilities through EW and CNO development.

Discussion of each core capability helps us comprehend joint IO career force challenges. "PSYOP has a central role in the execution of IO at all levels… As the information environment evolves the delivery means… are expanding from traditional print and broadcast… to internet, facsimile, text messaging, and other emerging media."[18] More than any other IO core capability, PSYOP requires cultural understanding and language training. PSYOP is a direct accession within the Army, with officers trained and retained as PSYOP professionals. The other services and US Special Operations Command (USSOCOM) use the Army PSYOP school to train their personnel.

MILDEC are "those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that" contribute to the friendly mission accomplishment.[19] MILDEC exploits the adversary's information systems, processes, and capabilities, and like PSYOP, is fundamental to IO. MILDEC requires formal training, though once trained, individuals may or may not serve in a deception position again. By the program's very nature, these operations are normally hidden from the broad military population.

OPSEC is the process of identifying essential elements of friendly information our adversaries could use to create an accurate picture of our forces, capabilities, and intentions—and denying them the same information. It is not a career field in any of the service, but rather a formal, managed program requiring annual training for all personnel.

EW includes three subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). "EW contributes to the success of IO by using maneuver, attack, and defense in a variety of combinations to shape, disrupt, and exploit adversarial use of the electromagnetic spectrum while protecting friendly freedom of action in that spectrum."[20]

EW core specialists perform a dynamic role during combat planning, ensuring constant deconfliction between exploitation versus denial. EW training serves as a joint IO training model, since Navy, Air Force, and Marine crews all receive basic EW training at the Navy's Pensacola facilities. In the Air Force, EW training follows initial navigator training, since AF electronic warfare officers are rated navigators. Additionally, the EA-6B is a joint EW platform utilizing all three services as mission crew. The Army is developing their EW program at three locations: EA at Fort Sill, Oklahoma—along with effects based operations in the fire and effects coordination cell; EP at Fort Knox, Kentucky; and ES at Fort Huachuca, Arizona.

CNO is comprised of computer network attack, computer network defense, and computer network exploitation. Our world has come to depend upon technological networks such as power grids, highways, water distribution, and information networks, for our very existence. "As the capability of computers and the range of their employment broadens, new vulnerabilities and opportunities will continue to develop … both to attack and exploit and adversary's computer system… (and) to identify and protect our own from similar attack and exploitation." [21]

We currently have no joint CNO doctrine, though the Joint Task Force for Global Network Operations (JTF-GNO) under USSTRATCOM is developing standard operating and reporting procedures. But JTF-GNO has no punitive authority to enforce either of these. And authority is key to any successful joint effort. While focused on joint IO training, this discussion requires an overview of respective services' approaches to IO training, since they must organize, train, and equip.

Service IO Approaches

The Army has embraced IO force development with the creation of IO career field (IOCF). The field comprises seven functional areas (FA): Information Systems (IS) Engineering, IS Management, Strategic Intelligence, Public Affairs, Space Operations, Simulation Operations, and Information Operations. The Information Operations (FA 30) is the integrating FA. Though the Army recognizes the same core, supporting, and related IO capabilities within joint doctrine, PSYOP and EW are not included in the Army IOCF!

The Army designates IO FA officers between their 5th and 6th years of service. The FA 30 IO training is 3 months long. Minimally, officers will not begin FA 30 training until they have qualified for promotion to captain (O-3) in their basic branch. Many will not serve in a FA 30 assignment until selected for major (O-4), and placed in the IOCF by a Career Field Designation BOArd. Only initial IO training is identified in the career path. The remainder of an Army IO career is comprised of IO assignments at increasing levels of responsibility starting at the maneuver brigade, then division through joint staff, and normal professional military education (PME) —unless an individual is selected to attend a civilian university instead of PME. The concept is to expose the officer to a variety of IO environments.[22] The Army's IOCF puts them farther ahead of the other services, but it doesn't provide for direct accessions as an FA 30.

The Air Force (AF) believes IO is integral to all operations. Air Force Doctrine Document 2-5, *Information Operations*, identifies three IO capabilities—influence operations, EW operations, and network warfare operations. Within influence operations they group military activities of PSYOP, MILDEC, OPSEC, counterintelligence, counterpropaganda, and public affairs—with the caveat "while a component of influence operations, (PA) is predicated on its ability to project truthful information to a variety of audiences." [23] Network warfare is broken into network attack, network defense, and network warfare support similar to CNO. EW is the same as joint doctrine.

The AF IO career force approach is also slightly different than the Army. Rather than an AF IO career field, the AF will create an IO career force from 19 existing career fields. Once IO trained, an officer's AF Specialty Code (AFSC) includes a special experience identifier (SEI) for tracking within the AF personnel system. These 19 career fields include related capability fields as electronic warfare officers (navigators), public affairs, and communications, along with combat operations fields such as pilots and air battle managers. The group also includes legal, behavioral science, research scientists, and the Air Force Office of Special Investigations to name a few. Officers would retain their primary career field, with an SEI to highlight IO experience.

From the AF perspective, the closest major weapons system associated with IO is the Aerospace Operations Center (AOC), thus they chose Air Combat Command (ACC) as IO lead major command. Air Education and Training Command (AETC) is evaluating IO courseware through a formal course development process. One significant difficulty: without a designated career field, there is no Air Staff general officer advocate for funding, doctrine, training, and organization issues. An IO general officer steering group is reviewing this issue. While working the AF IO mission essential task list, ACC is making a major effort to balance resources while providing minimum IO training competency. [24]

US Navy doctrine recognizes the same core capabilities as joint doctrine. The Navy's IO warrior development is in "mid-stride." In 1994, Commander Naval Security Group became Executive Agent for IW/C2. In 2005, they converted all officer "cryptologists" to "information warfare," following IO direction in the DPG 04-06 and the DOD *IO Roadmap*. The Navy has significant EW and CNO capabilities, compared to lesser capabilities in OPSEC and MILDEC. They continue working a job task analysis to determine which positions should be manned by what type IO career officer, and what training will help them succeed at each respective level. Aside from core capability area training in traditional

SIGINT and EW disciplines, the Navy's beginning IO planners training is a two week staff course. Time and funding permitting, they are attempting to utilize available Joint Forces Staff College IO courses. Additionally, the Navy has a unique IO challenge due to their funding lines. Major program funding is tied to platforms. There is no dedicated single resource sponsor to sponsor investment, since IO is not unique to a submarine, aircraft or surface vessel. In the terms of EW technology, the Navy is building new architectures which can be used across multiple major programs with only minor software modifications, to ensure EW and IO integration. Most dedicated IO expertise is found in the IW officer community and enlisted cryptologic technician community. Officers and enlisted personnel from traditional aviation, surface, and subsurface warfare communities can be assigned to IO billets, either in a capability area or as an IO planner, but do not normally count themselves as part of the IO Career Force. The major exception is the EA-6B Prowler community, which counts EW as their primary mission area, and therefore as IO Career Force members. While IO planners may come from unrestricted line officers (URL), these normally only serve one tour in the IO community. While a URL officer has combat focus, they may not have an IO skill set or expertise. Thus, the overall Navy concept is to use IO capability specialists in IO planner positions, vice creation of a new IO "generalist" career field.[25]

"The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities… (and) a solid foundation of education and training is essential to the development of a core competency."

While the Marines have IO officer military occupational specialties (MOS), they take a slightly different broad IO view. Information operations are not simply another arrow in the MAGTF (Marine Air-Ground Task Force) commander's quiver, but a broad-based integrative approach that "makes the bow stronger." This distinction is key to the belief IO does not, and will not, replace any time-tested warfighting functions, rather it will enable each of them. Thus, the Marine Corps' approach to IO and information-oriented activities would best provide tailored application of combat power to meet the joint force commander's needs.[26]

The Marines have a robust cadre of electronic warfare officers. A small number have graduated from the NPS with a master's degree in Information Warfare. These officers were initially designated an information warfare officer MOS, followed by IO officer, and finally Technical IO officer (MOS 9634) in 2005, to reflect NPS course changes.[27] The Marines use IO Technical officers in positions requiring a technical background such as requirements, plans, and policies. Additionally, they created an IO Staff officer specialty (MOS 9934) in 2004, in response to DPG direction to create an IO career force. The designator indicates an IO officer on a MAGTF or other staff position. The 9934 is an "additional" MOS, as officers in this code continue to serve in their primary MOS with periodic tours in IO. These officers must complete a course of study at least two weeks in length (such as the Navy, JFSC, or Army school), plus serve a minimum of 6 months in an IO billet performing IO duties. The IO Technical officer and IO Staff officer are IO planners. Marine capability specialists are defined through their area of expertise, such as an EA-6B pilot, CNO, or PSYOP. The Marines are also adding two new company grade and enlisted IO specialty codes, to better track IO experience and expertise.[28]

In summary, all services are working diligently on their respective IO career force. Each is a constantly moving target requiring constant IO optimization changes, yet none have direct accession into the IO planner career field. There are direct accessions into some of the core capabilities, yes—but not IO planners. However, joint combatant commanders expect IO planners to lead every IO cell around the world. Ideally, planners should have a technical IO background, to fully understand IO execution and integration. If IO is a core military competency, shouldn't an IO planner be a direct accession into the IO career field? The problem stems from too little IO history, and too much specific capability history. With the DOD direction to establish an IO career force, the services have merged several independent but related activities. Each core capability brings some inherent baggage and inertia along with it. The IO forge is working: we've smelted the "ores," but an IO alloy hasn't bonded. It might have taken less time to start from a clean slate, but the military could not afford to lose the history, skill, experience, and knowledge in the core capabilities.

Discussion

The civilian leadership has thrown down the gauntlet. "The QDR identified capability gaps in each of the primary supporting capabilities of… Information Operations … to close those gaps, the Department will focus on organizing, training, equipping, and resourcing the key communication capabilities. This effort includes developing new tools and processes for assessing, analyzing, and delivering information to key audiences, as well as improving linguistic and cultural competence … with the goal of achieving a seamless communication across the US Government." [29] JP 3-13 states, "The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD… At each level of command, a solid foundation of education and training is essential to the development of a core competency." [30] It's a Catch-22 situation. "Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation."[31]

JP 3-13 identifies three basic tenets of IO education and training: 1) the IO career force should consist of both core capability specialists (EW, PSYOP, and CNO) and IO planners; 2) initial capability specialist training and education requirements are Service and capability specific; and 3) IO planners are required at both the component and joint level. Joint IO training directs joint doctrine and policies, and assumes a solid foundation of Service-level IO training.[32] But this hasn't happened yet. "Within DOD, over 400 IO-related courses currently provide knowledge and skill training to IO planners and capability specialists. Some... are redundant. There is neither a formal DOD-wide standard on how IO knowledge and skills are trained, nor a single formal plan to ensure that information presented by different organizations for similar course objectives are standardized."[33]

While new JP 3-13 and DODIs now provide joint IO doctrine, many current courses are service specific. Thus, most developed without any formal process to ensure consistent objectives and content. Additionally, since these courses aren't standardized, we see some service rivalry with regard to curriculum. The previously noted lack of joint doctrine, and still developing service doctrine, contributes to constantly evolving IO tactics, techniques, and procedures (TTPs). This wastes limited funds for the IO community with redundant courses, instructors, and materials. It breeds a lack of confidence in the general military population because of differing knowledge and skill levels and different TTPs for implementing IO. This impacts leaders and their willingness to release personnel for initial or advanced training. Services cancelled previous IO courses because commanders were unwilling to pay for, or allow personnel to attend courses exceeding three weeks. Additionally, the inconsistency makes IO a harder "sell" for future IO career force recruits. Now that USD(I) has directed IO become a core competency, service doctrine should solidify and align with joint doctrine. The services are responsible for training their IO career force and general populations, based upon identified joint force mission requirements. Service-wide military training should account for the nature of the information environment, and that individual actions can affect the view of foreign populations.[34] IO impacts perceptions, and an adversary or local media can destroy positive perceptions in an instant, if given the opportunity by a military member's inadvertent cultural faux pas or outright criminal act. The Sec Def and services realize language and cultural skills are critical to IO. This is reflected in the QDR, and the push for increased language training outside that already utilized within the intelligence community. "Misperception and misunderstanding are complicated and reinforced when joint forces do not have sufficient language and cultural skills to communicate effectively with the populations among whom they operate."[35]

IO Warriors must understand the cultural environment. (Defense Link)

One of our greatest challenges is educating warriors on how to think about IO; it requires very detailed analysis and skilled synthesis, fueled by specific subject matter expertise and knowledge. IO requires its practitioners to view problems and challenges as holistic and related, instead of isolated. Each part of IO relates to the others, just as actions in one part of the world in one domain can cascade into other parts of the world and in other domains. IO education must give everyone a broad appreciation of how different cultures affect the ways people think, plan, and interpret outcomes. IO planners also need sufficient education to conducting sophisticated wargaming, to let them go back and forth from the mind of the friendly commander to the mind of other participants in conflict, all of whom influence friendly COAs.[36]

IO warriors must be able to detect patterns and opportunities within the information environment. This requires increasingly in-depth instruction appropriate to the leadership level. Such training requires a solid foundation and continual education, reinforced and enhanced throughout a career. What strategy should be reinforced in the curriculum? IO as influence and technical, offensive and defensive, denial and exploitation—or lethal and non-lethal? All must be addressed.

Not only is the standardization of current knowledge an issue, another (in particular for CNO) is the pace of technology and related education. Moore's Law states computing power doubles every 18 months; fiber law claims communications capacity doubles every 9 months; and disk law notes storage capability doubles every 12 months.[37] One would think, even with the pace of technology, we know most of what we need to know about computer networks. We don't. Future operations will depend on many other types of networks. While we depend upon networks, our fundamental understanding of networks is primitive. In *Network Science*, commissioned by the BOArd on Army Science and Technology, researchers found "the components of modern communication and information networks are the result of technologies… emanating from physics, chemistry, and materials science. Their assembly into networks, however, is based largely on empirical knowledge rather than on a deep understanding of the principles of network behaviors gained from an underlying science of networks." [38] Physical networks are the Internet, highways, air transportation networks, and global financial networks. Biological networks are our bodies metabolic and genetic expression systems. Social networks include businesses, governments, and military organizations. "The military's dependence on interacting networks in the physical, information, cognitive, and social domains is clear from its effort to transform itself into a force capable of network centric operations (NCO)."[39] But there is a gap between the military vision of NCO and our current network knowledge, particularly the impact of biological and social networks on physical networks. How do you standardize the current education and training when the environment in question is constantly changing?

From these discussions, we can begin to grasp the difficulties of IO training challenges. "The integration envisioned as not mere deconfliction, but the synchronization and harmonization of activities whose resulting effect is significantly greater than the sum of the individual components." [40] DODI 3608.12 tasked the National Defense University to direct JFSC to develop and conduct joint IO courses, and the school currently offers one and four week versions. The objective of the Joint IO Orientation Course (JIOOC) is to educate and train personnel in joint IO basics, with primary emphasis at the Combatant Command level. The focus is joint IO doctrine and DOD IO policy guidance as they apply to the operational level of joint warfare. JIOOC is relevant to those serving in support of IO cells and other staff positions requiring basic joint IO knowledge. The Joint Information Operations Planners Course (JIOPC) is four weeks long, and establishes a common level of understanding for IO planners and capability specialists who will serve in joint operational-level IO billets. JIOPC includes JIOOC material, and adds three weeks of intensive experience in the Joint Planning Process. It is a prerequisite for personnel assigned to the Joint IO career force.[41] Additionally, DODI 3608.12 tasked the Naval Postgraduate School (NPS) to establish a DOD IO Center of Excellence, and to develop and maintain a graduate level joint IO education program. The Masters of Science in IO is 18 months in length and has been offered for two years (as of 2006). Graduates are taught to employ information in support of full spectrum dominance by taking advantage of information technology, exploiting growing worldwide dependence on automated information systems, and capitalizing on near real time global dissemination of information to affect adversary decision cycles. This capability will be possible only after students develop a thorough understanding of the enduring nature of war. The program is "designed for both the specialist who will be assigned to an information operations position and the generalist who will be assigned to an operations directorate. The curriculum includes: a core of military art and operations; the human dimension of warfare (psycho-social), analytical methods; and a technical sequence customized for each student. Additionally, each student has an elective sequence designed to further develop an in-depth understanding of joint IO."[42] An additional confusion factor is NPS's masters degree in Information Warfare program, which grants EW personnel a technical degree. Though placing significant demands for graduates from the course, neither the COCOMs nor services have yet established a "demand signal" for the degree program.

Based upon the complex understanding required, an IO warrior can't learn enough in four weeks to analyze and synthesize everything needed to truly orchestrate an IO campaign. Plus, commanders are reluctant to release someone for 18 months to attend the limited NPS allotments. The NPS program is treated as an Intermediate Service School or Intermediate Developmental Education program, attended by O-3s in lieu of a masters degree, or O-4/O-5s instead of their respective service schools. The program is limited to 20 students, five from each service, per course. Currently the Joint Staff is considering whether the NPS course should be reduced to a 10 month program. Meeting standardized learning objectives should set course length, not the number of days a command is willing to release a senior member for temporary duty or training.

Once an individual has IO knowledge, they need train how they will fight. "Knowing is not enough; we must apply. Willing is not enough; we must do." [43] This requires application in exercises, and joint ones in particular. Historically, IO is rarely used in exercises though it is becoming more common. Too often an IO capability specialist or planner's first attempt is a real world situation, after he or she is thrown onto a staff without the necessary background. The lack of proper support or background typically makes these attempts frustrating and insufficient.

These challenges are but a few of those facing the IO career force. DOD and the Joint Staff have given the services a new IO vector. The complex systems and rapid processing speeds, brought on by the information age, drive this new direction. Speed is transitioning the world out of the information age to a conceptual age. Society is moving from knowledge workers to creators and empathizers. Affluence, technology, and globalization are all enabling this transition. [44] The following recommendations help address these challenges, and indicate those the IO community is currently researching—or could readily implement.

Recommendations

Education and Training

First, we must have an executive agent for joint IO training. With the release of DODI 3608.12, USSTRATCOM is now the operational advocate for Joint IO education—one of several new STRATCOM missions. They are working with the Joint Staff to standardize IO inputs for the universal joint task list (UJTL) and mission essential task list (METL). Simply put, DOD must fund this new mission, as vision without funding is an hallucination.

IO education and training must be standardized DOD-wide, and adaptable enough to flow with the changes. This requires an extended review of all current IO-related education, and skill training for both IO capability specialists and planners. A full joint IO training analysis is necessary to develop an effective education and training program.[45] "Desired learning objectives need to be standardized… for creating effective and comprehensive IO education and training."[46] We must consolidate redundant courses, and jointly utilize those remaining to establish a solid IO foundation across the services. A single, all-service entry level joint IO technical school, similar to the EW school at Pensacola, would immediately increase knowledge standardization. Students would attend a service-specific school following this course.

IO training needs to be increased, or in some cases included, in all PME and leadership development courses. Training must also provide DOD commanders and leaders the means to effectively integrate IO and IO warriors into their organization, at all levels. All IO courses must teach, and strive to improve, joint IO tools and software. A common DOD-wide tool kit would allow IO warriors to merge into any theater IO cell with only area specific spin up, increasing the IO capability—and ultimately the combat capability—of the respective joint command.

Further, IO needs live exercise learning environments, command post exercises, and simulations. *(Editors note: see the IO Range article by Robert Sabo, page 8.)* These must involve full spectrum IO in the planning stage, all execution phases, and through the after action report. Next, create a joint IO opposing force (OPFOR). No enemy is static, so realism requires an adversary who responds or anticipates and prepares a counter-thrust—an IO coup fourré.[47] A fully trained, educated, scalable, and responsive IO OPFOR, complete with all necessary privileges to incorporate all five core capabilities in a synergistic effect, could provide a realistic full-spectrum threat representation.[48]

These education and training recommendations maximize limited funds and facilities, and increase standardization of knowledge and application. Standardization is "essential to integrating IO TTPs into joint exercises and improving real-world IO performance." [49] As noted earlier, true understanding comes from application of knowledge.

Officer Accession

The IO planner career field should be a direct accession, with IO capability specialists as initial accessions in certain functional areas. IO planners tend currently spend their early careers in another primary specialty field. Some may come from EW, PSYOP, or CNO backgrounds, but that is currently the exception rather than the norm. The complexity of the environment, and the extensive IO warrior knowledge requirements demand direct accession into an IO career field. Career broadening into a combat arms field should be part of the career progression, not the other way around.

DOD should use IO planners in those positions where they make the most impact. This requires identification of critical joint, service, and combatant command IO positions. This is extremely important in career force growth, and spreading the IO culture across the DOD. The BOA working group is staffing an action to accomplish just such a task.

Advocacy

DOD is starting to see O-6 and O-7 advocacy at the joint and combatant command level. This is a great start. True advocacy, and thereby funding, must come from a senior service-level FO/GO advocate, since the services control the major portion of the DOD budget. Without three and four star support, IO will limp along through the diligent efforts of "iron majors" at the operational and tactical level, but languish at the strategic level. The IO community requires strategic direction and advocacy to improve and ease access.

Though a recent creation, the BOA is making strong forward progress. Their current major task is identifying joint IO billets, and respective education requirements for each.

The final recommendation is ironic: Use IO to improve IO. Current IO personnel don't use IO to promote or advance IO. In fact, to a certain extent IO is its own worse enemy. Many IO programs are compartmentalized, and even basic IO documents are "close hold," limiting visibility to the core of the military. Without at least some visibility into the IO world, why would a new officer want to become an IO warrior?

Conclusion

DOD is moving in the right direction. The doctrine and vector provided in the latest guidance lay the foundation for a bright IO future. To realize that future requires hard work, general officer advocacy, standardization of IO training, education, and tools, and using IO to spread the IO message. Military services must align and support joint IO to defeat the existing resistance to IO as a core military competency. Without these improvements, IO will continue to have "potentially marked differences in the knowledge and skill level of IO personnel from mission to mission and organization to organization."[50] We can overcome these differences, but this requires guidance from senior leadership. The IO BOArd of Advisers is the best avenue to establish joint requirements and direction. By bringing service IO together, and aligning strong IO technical backgrounds with the other soft power IO capabilities, DOD will develop joint warriors capable of executing IO as a core military competency, and ensuring US information dominance.

Notes

[1] Sun Tzu, The Art of War, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 77.

[2] Hebert, Adam J., "Information Battleground," Air Force Magazine, Vol. 88, No. 12 (December 2005); available from http://www.afa.org/magazine/Dec 2005/1205info.html; Internet; accessed 25 Feb 2006.

[3] Under Secretary of Defense for Intelligence, *Information Operations Career Force*, DODI 3608.11 (Washington, D.C., Department of Defense, 4 Nov 2005), 1.

[4] Stephen R. Covey, *The 7 Habits of Highly Effective People* , (New York: Fireside, 1989), 97.

[5] DODI 3608.11, 2.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Under Secretary of Defense for Intelligence, "Joint Information Operations (IO) Education," DODI 3608.12 (Washington, D.C., Department of Defense, 4 Nov 2005), 3-6.

[10] Director, Joint Staff, *Information Operations*, Joint Publication 3-13 (Washington, D.C. Joint Staff. February 2006), GL-9.

[11] Ibid., x.

[12] Ibid., iii.

[13] Ibid., ix.

[14] Ibid., I-1.

[15] Ibid.

[16] Ibid., I-2.

[17] Ibid., I-9.

[18] Ibid., II-2

[19] Ibid., 16.

[20] Ibid., II-4.

[21] Ibid., II-5.

[22] US Department of the Army, *Commissioned Officer Professional Development and Career Management*, Army Pamphlet 600-3 (Washington, D.C.: US Department of the Army 600-3, 28 December 2005), 227; available from http://www.apd.army.mil/pdffiles/p600_3.pdf; Internet; accessed 13 April 2006.

[23] HQ AFDC/DR, *Information Operations*, AFDD 2-5 (Washington D.C., HQ USAF, 11 Jan 05), 5.

[24] Mr. Paul Scott, Air Combat Command A3I, telephone interview by author, 24 February and 6 April 2006.

[25] CAPT Stephanie Helm, N3IO, IO Branch Chief, telephone interview by author and e-mail, 13 April 2006.

[26] This concept was first published in an article by Edward Hanlon, Jr., LtGen, USMC, Marine Corps' Concepts and Programs Document, (Washington D.C., HQ USMC, 2006) 39.

[27] HQ USMC, *Marine Occupational Specialties Manual*, MCO P1200.16, (Washington D.C., HQ USMC, 18 April 2005), 1- 108, 1-144.

[28] Col J. R. Wassink, HQ USMC, Branch Chief PLI, telephone interview by author and emails, 6 -11 April 2006.

[29] Secretary of Defense, *Quadrennial Defense Review Report*, (Washington D.C., Office of the Secretary of Dense, 6 Feb 2006), 92.

[30] JP 3-13, VII-1.

[31] Ibid.

[32] Ibid., VII-2.

[33] Information Assurance Technology Analysis Center (IATAC), *The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy* (Falls Church: IATAC – Booze Allen), 20.

[34] JP 3-13, VII-2.

[35] Ibid.

[36] Ibid.

[37] Al Shaffer, "Transitioning S&T Programs" briefing slides presented to the Defense Systems Acquisition Management Course, 17 June 2004; available from http://proceedings.ndia.org/402C/402C_Shaffer.pdf; Internet, accessed 7 Apr 2006.

[38] The National Academy of Science, *Network Science,* (Washington D.C.: The National Academy Press, 2005), 26.

[39] Ibid., 1.

[40] COL David J. Smith, ed., *Information Operations Primer*, (Carlisle Barracks, PA: US Army War College, January 2006), 1.

[41] The Information Operations Division Home Page, available from http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/default.asp; Internet; accessed 7 April 2006.

[42] The Graduate School of Operations and Information Sciences Home Page, available from http://www.nps.navy.mil/GSOIS/programs/programs_009.htm ; Internet; accessed 7 April 2006.

[43] Bruce Lee, Quoteworld, available from http://www.quoteworld.org/quotes/8155; Internet; accessed 7 April 2006.

[44] Daniel H. Pink, *A Whole New Mind*, (New York: The Penguin Group, 2005), 49.

[45] IATAC, 53.

[46] Ibid., 32.

[47] Coup Fourré: a French fencing term for counter-thrust where one fencer parries his opponent's thrust and counter attacks in the same maneuver.

[48] IATAC, 76.

[49] Ibid.

[50] Ibid., 53.

Lt Col (Col Select) Jim "Dill" Pickle, US Air Force, serves as Chief, Program Management Branch, Operational Support Modernization Division, Warfighting Integration and Chief Information Officer Directorate (SAF/XC) at the Pentagon. Previous assignments include the Joint Staff J-3 Readiness Branch, Commander 623rd Air Control Flight, and 607th Air Support Operations Group Director of Operations. He has served as an AWACS Senior Director, Mission Crew Commander, and Detachment Commander during Operation SOUTHERN WATCH. He holds a BA in Broadcasting from John Brown University and Masters degrees from Webster University, Air Command and Staff College, and Army War College. Readers may contact him at james.pickle@pentagon.af.mil